Data Security

Lecture No. (7)

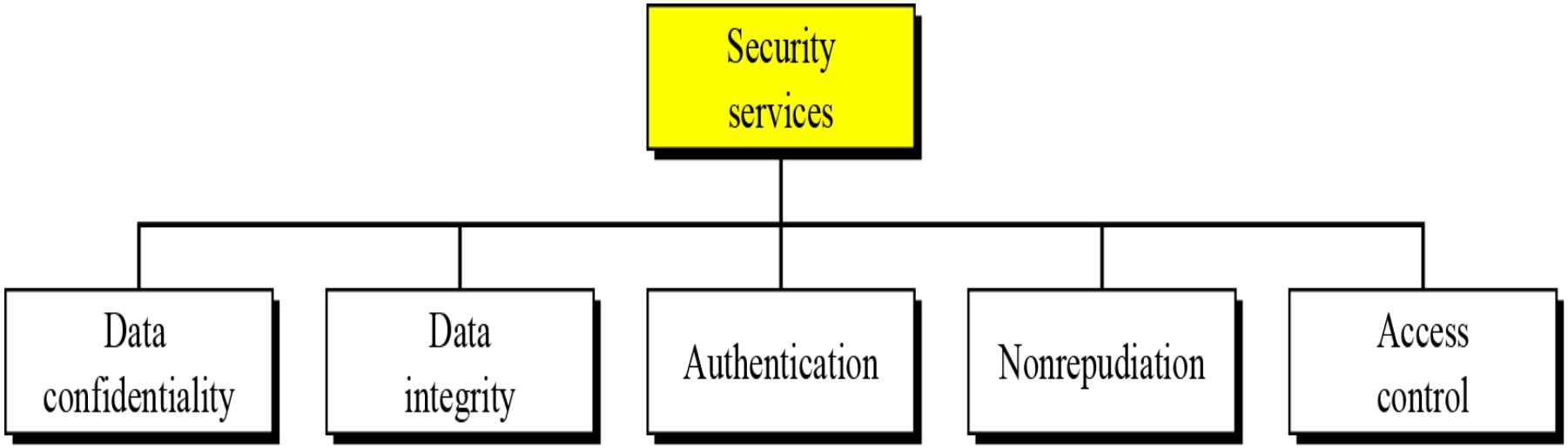
Dr/ Roayat Ismail

Objectives

1. To know how we can achieve data integrity by using hash function.
2. To define a digital signature.
3. To define security services provided by a digital signature.
4. To discuss RSA digital signature.

Security services

Standards have been defined for security services to achieve security goals and prevent security attacks. The figure shows the taxonomy of the five common services.



Security services

How security services can be achieved?

1. Confidentiality (with encryption).
2. Integrity (with hash functions).
3. Authentication (with MAC function).
4. Non-repudiation (with digital signature).

MESSAGE INTEGRETY

Integrity need a way to ensure that data arrives at destination in its original form as sent by the sender and it is coming from an authenticated source.

It can be achieved by using hash function.

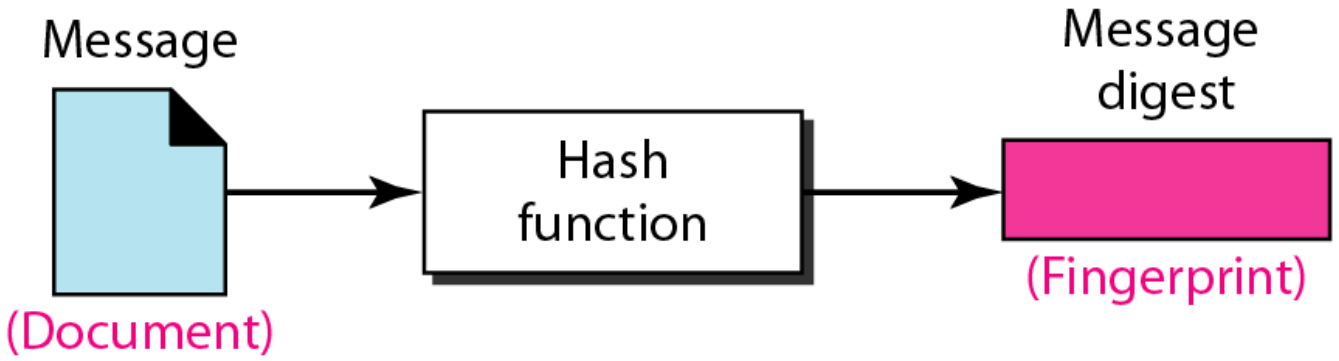
Hash functions

Hash functions

A **hash function** is a mathematical function that generally has the following three properties:

1. **Condenses arbitrary long inputs into a fixed length output (compression)**
   - You enter as much data as you want into the function, and it gives an output (or **hash**) that is always the same fixed length.
   - In general this hash is much smaller than the data that was put into the function.
   - Because the hash is a smaller thing that represents a larger thing, it sometimes referred to as a **digest**, and the hash function as a **message digest function**.

Message and message digest



Notations:

m: message

H(m): message digest of m by using hash function H()

The digest created by a cryptographic hash function is normally called a **modification detection code (MDC)**.

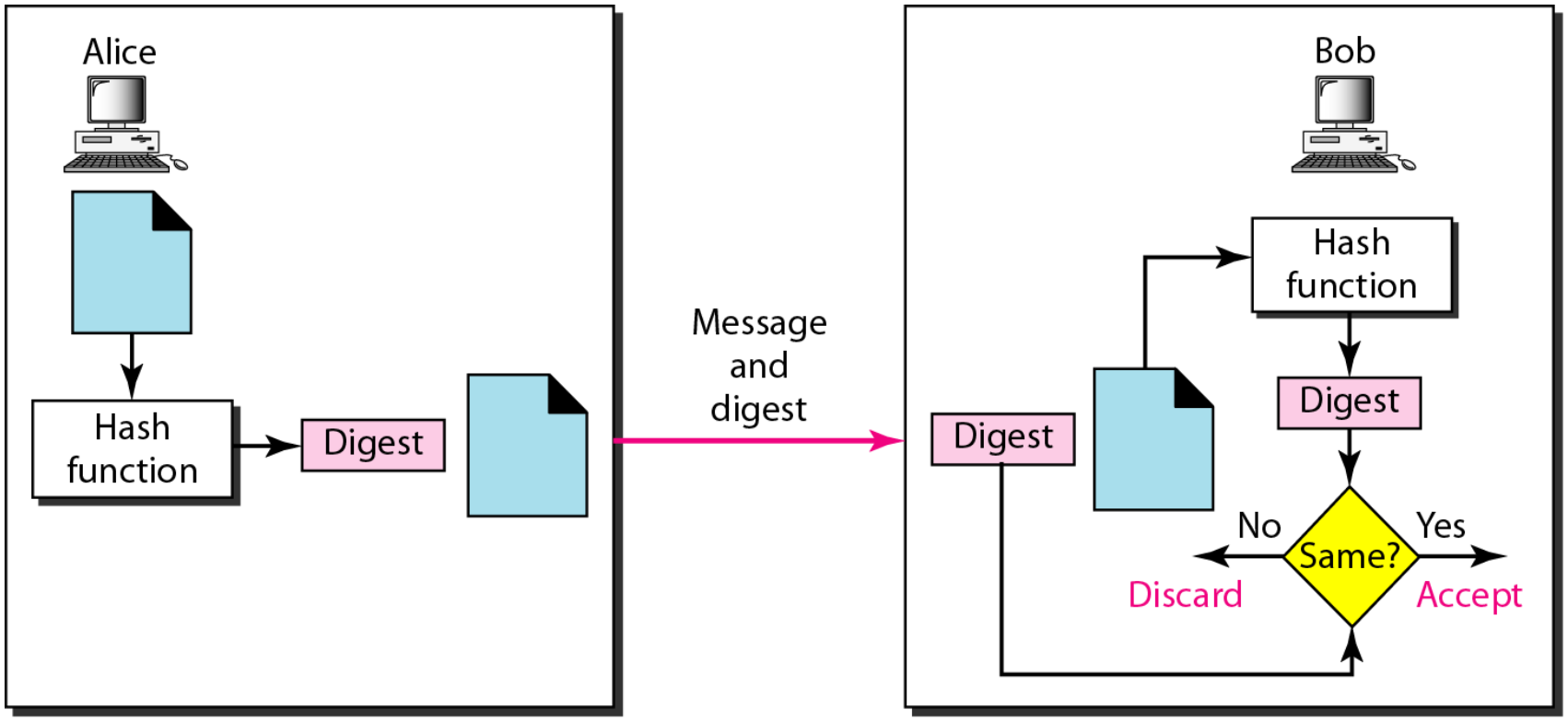
Properties of hash functions

2. **It is a one-way function:**
   - The hash function should be easy to compute, but given the hash of some data it should be very hard to recover the original data from the hash.
3. **Collision free:**

It is hard to find two inputs with the same output

- It should be hard to find two different inputs (of any length) that when fed into the hash function result in the same hash.

Checking data integrity by using hash function



Well Known Hash Functions

- MD5
  - output 128 bits
  - collision resistance completely broken by researchers in China in 2004
- SHA1
  - output 160 bits
  - no collision found yet, but method exist to find collisions in less than 2^80.
- SHA2 (SHA-224, SHA-256, SHA-384, SHA-512)
  - outputs 224, 256, 384, and 512 bits, respectively
  - No real security concerns yet.

MESSAGE AUTHENTICATION

A hash function cannot provide authentication. The digest created by a hash function can detect any modification in the message, but not authentication.

A message digest guarantees the integrity of a message—it guarantees that the message has not been changed. A message digest, however, does not authenticate the sender of the message. When Alice sends a message to Bob, Bob needs to know that the message is really from Alice

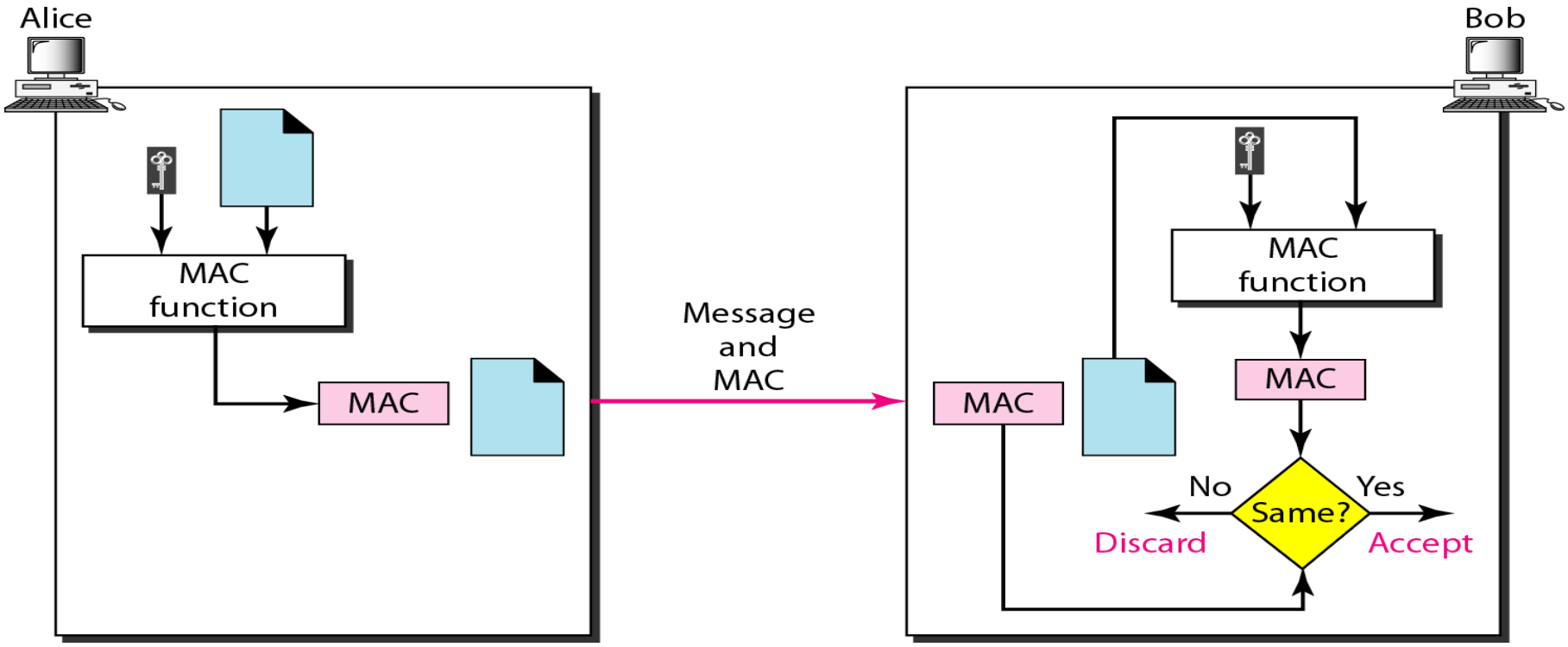
Message authentication

To provide message authentication, Alice needs to provide proof that it is she who is sending the message and not an impostor. A message digest cannot provide such a proof. What we need for message authentication is a message **authentication code (MAC)**.

MAC (message authentication code): can be used to ensure both integrity and authentication.

Message authentication code (MAC)

To ensure the integrity of the message and authenticate its origin, we need to change an MDC to a MAC. The difference is that the latter includes a secret between Alice and Bob.



Message authentication code

Non-repudiation:

In a cryptographic context, the word *repudiation* refers to the act of disclaiming responsibility for a message.

Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

A message's recipient may insist the sender attach a signature in order to make later repudiation more difficult, since the recipient can show the signed message to a third party (eg, a court) to reinforce a claim as to its signatories and integrity.

Non-repudiation (Example)

- Alice orders 100 shares of stock from Bob
- Alice **signs** order with her private key
- Stock drops, Alice claims she did not order
- Can Bob prove that Alice placed the order?
- **Yes!** Only someone with Alice's private key could have signed the order
- This assumes Alice's private key is not stolen.
- Non-repudiation can be achieved only by digital signature.

DIGITAL SIGNATURE

When Alice sends a message to Bob, Bob needs to check the authenticity of the sender; he needs to be sure that the message comes from Alice and not Eve. Bob can ask Alice to sign the message electronically. In other words, an electronic signature can prove the authenticity of Alice as the sender of the message. We refer to this type of signature as a digital signature.

Comparison between conventional signatures and digital signatures.

1. Inclusion
2. Verification Method
3. Relationship
4. Duplicity

1. Inclusion

A conventional signature is included in the document; it is part of the document.

But when we sign a document digitally, we send the signature as a separate document.

2. Verification Method

For a conventional signature, when the recipient receives a document, she compares the signature on the document with the signature on file.

For a digital signature, the recipient receives the message and the signature. The recipient needs to apply a verification technique to the combination of the message and the signature to verify the authenticity.

3. Relationship

For a conventional signature, there is normally a one-to-many relationship between a signature and documents. For a digital signature, there is a one-to-one relationship between a signature and a message.

4 . Duplicity

In conventional signature, a copy of the signed document can be distinguished from the original one on file. In digital signature, there is no such distinction unless there is a factor of time on the document.

What is Digital Signature?

- Hash value of a message when encrypted with the private key of a person is his digital signature on that e-Document
  - Digital Signature of a person therefore varies from document to document thus ensuring authenticity of each word of that document.
  - As the public key of the signer is known, anybody can verify the message and the digital signature

Digital Signatures

Each individual generates his own key pair

[Public key known to everyone & Private key only to the owner]

Private Key – Used for making digital signature

Public Key – Used to verify the digital signature

RSA Key pair

(including Algorithm identifier)

[2048 bit]

Private Key

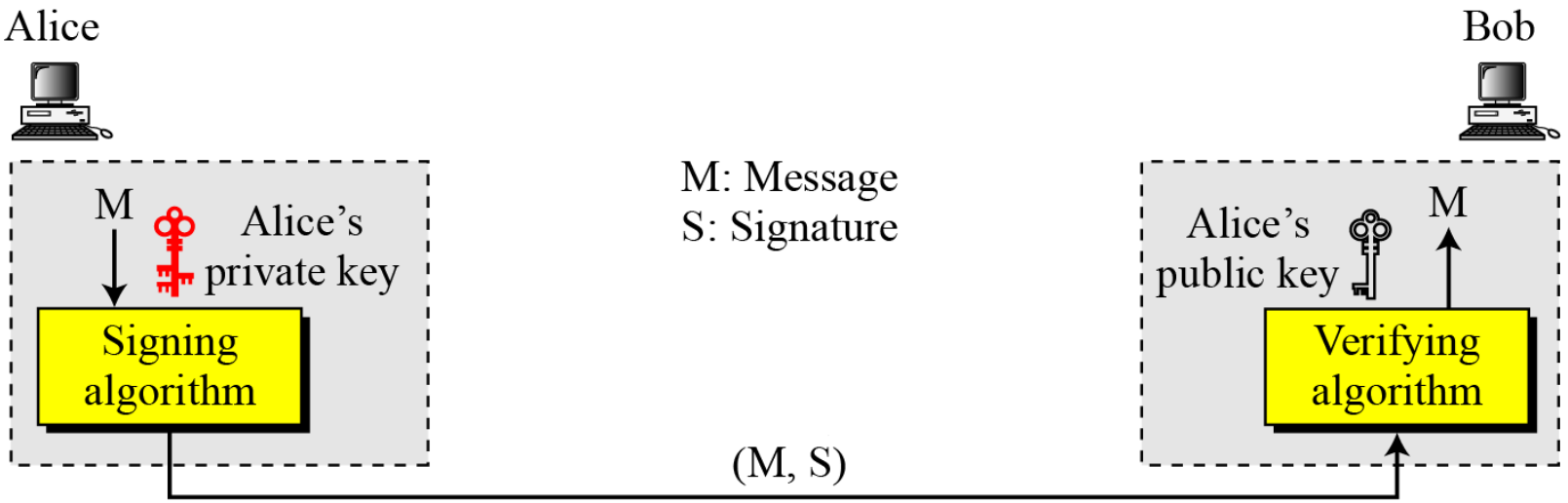
```
3082 010a 0282 0101 00b1 d311 e079 5543 0708 4ccb 0542 00e2 0d83 463d e493 bab6
06d3 0d59 bd3e c1ce 4367 018a 21a8 efbc ccd0 a2cc b055 9653 8466 0500 da44 4980
d854 0aa5 2586 94ed 6356 ff70 6ca3 a119 d278 be68 2a44 5e2f cfcc 185e 47bc 3ab1
463d 1ef0 b92c 345f 8c7c 4c08 299d 4055 eb3c 7d83 deb5 f0f7 8a83 0ea1 4cb4 3aa5
b35f 5a22 97ec 199b c105 68fd e6b7 a991 942c e478 4824 1a25 193a eb95 9c39 0a8a
cf42 b2f0 1cd5 5ffb 6bed 6856 7b39 2c72 38b0 ee93 a9d3 7b77 3ceb 7103 a938 4a16
6c89 2aca da33 1379 c255 8ced 9cbb f2cb 5b10 f82e 6135 c629 4c2a d02a 63d1 6559
b4f8 cdf9 f400 84b6 5742 859d 32a8 f92a 54fb ff78 41bc bd71 28f4 bb90 bcff 9634
04e3 459e a146 2840 8102 0301 0001
```

Public Key

```
3082 01e4 f267 0142 0f61 dd12 e089 5547 0f08 4ccb 0542 00e2 0d83 463d e493 bab6
0673 0d59 bf3e c1ce 4367 012a 11a8 efbc ccd0 a2cc b055 9653 8466 0500 da44 4980
d8b4 0aa5 2586 94ed 6356 ff70 6ca3 a119 d278 be68 2a44 5e2f cfcc 185e 47bc 3ab1
463d 1df0 b92c 345f 8c7c 4c08 299d 4055 eb3c 7d83 deb5 f0f7 8a83 0ea1 4cb4 3aa5
b35f 5a22 97ec 199b c105 68fd e6b7 a991 942c e478 4824 1a25 193a eb95 9c39 0a8a
cf42 b250 1cd5 5ffb 6bed 6856 7b39 2c72 38b0 ee93 a9d3 7b77 3ceb 7103 a938 4a16
6c89 2aca da33 1379 c255 8ced 9cbb f2cb 5b10 f82e 6135 c629 4c2a d02a 63d1 6559
b4f8 cdf9 f400 84b6 5742 859d 32a8 f92a 54fb ff78 41bc bd71 28f4 bb90 bcff 9634
04de 45de af46 2240 8410 02f1 0001
```

Need for Keys

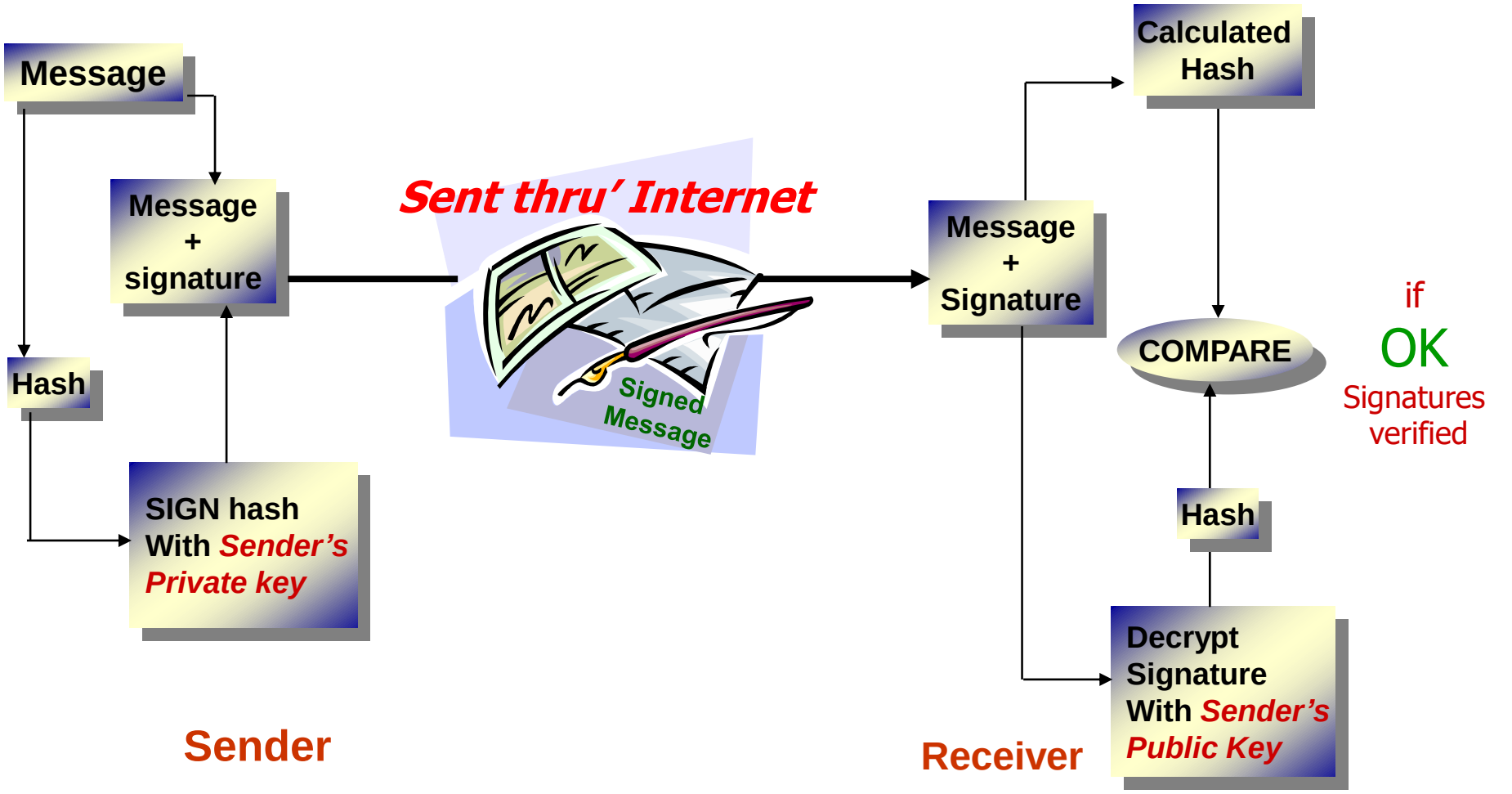
Adding key to the digital signature process



Note

A digital signature needs a public-key system. The signer signs with her private key; the verifier verifies with the signer's public key.

Signing *the Digest*



We use the term **signer** for an entity who creates a digital signature, and the term **verifier** for an entity who receives a signed message and attempts to check whether the digital signature is "correct" or not.

While data confidentiality has been the driver behind historical cryptography, digital signatures could be the major application of cryptography in the years to come.

Note

A cryptosystem uses the private and public keys of the receiver: a digital signature uses the private and public keys of the sender.

3 SERVICES

A digital signature can directly provide :

1. Message Authentication
2. Message Integrity
3. Nonrepudiation

But it can not provide confidentiality.

1. Message Authentication

A secure digital signature scheme, like a secure conventional signature can provide message authentication.

Note

A digital signature provides message authentication.

When ownership of a digital signature private key is bound to a specific user, a valid signature shows that the message was sent by that user.

2 . Message Integrity

The integrity of the message is preserved even if we sign the whole message because we cannot get the same signature if the message is changed.

Note

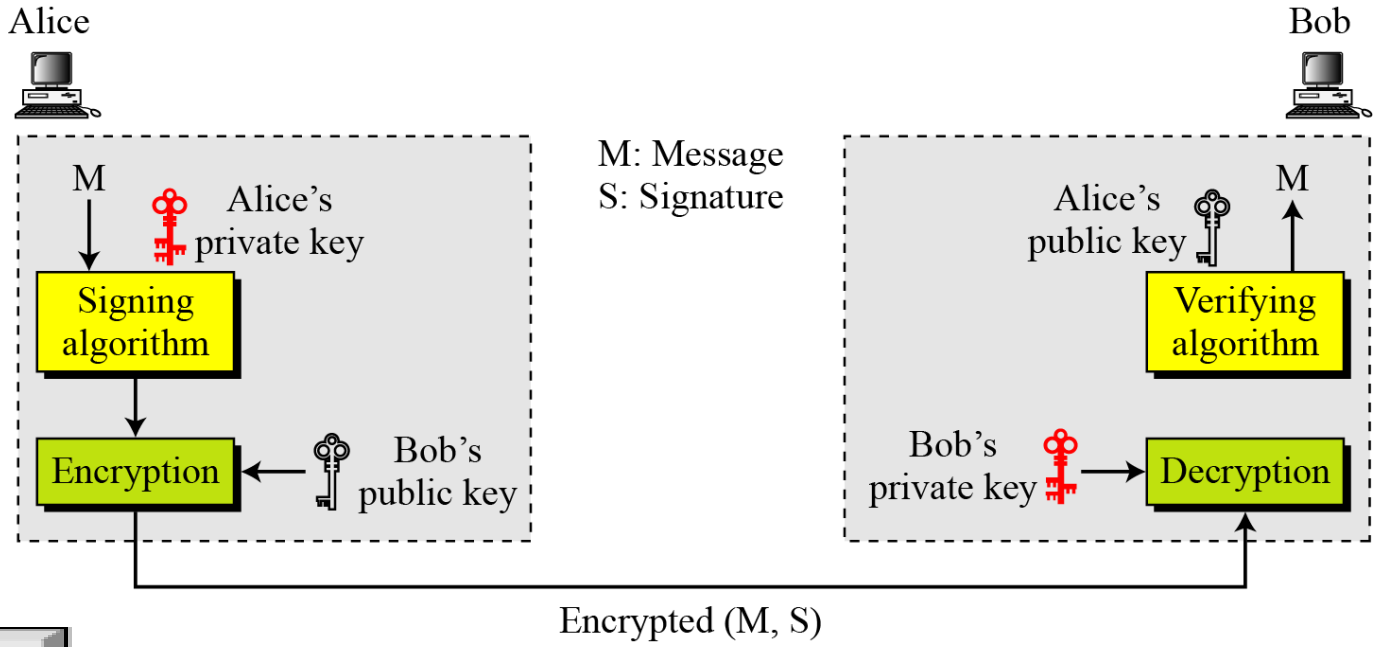
A digital signature provides message integrity.

3. Nonrepudiation

In digital signature, a message is signed with the sender private key which is uniquely used by him. So he can not deny signing it. So digital signature provides nonrepudiation.

4. Confidentiality

Adding confidentiality to a digital signature scheme



Note

A digital signature does not provide privacy. If there is a need for privacy, another layer of encryption/decryption must be applied.

5 DIGITAL SIGNATURE SCHEMES

Several digital signature schemes have evolved during the last few decades. Some of them have been implemented.

1. RSA Digital Signature Scheme
2. ElGamal Digital Signature Scheme
3. Schnorr Digital Signature Scheme
4. Digital Signature Standard (DSS)
5. Elliptic Curve Digital Signature Scheme

1. RSA digital signature

Key Generation

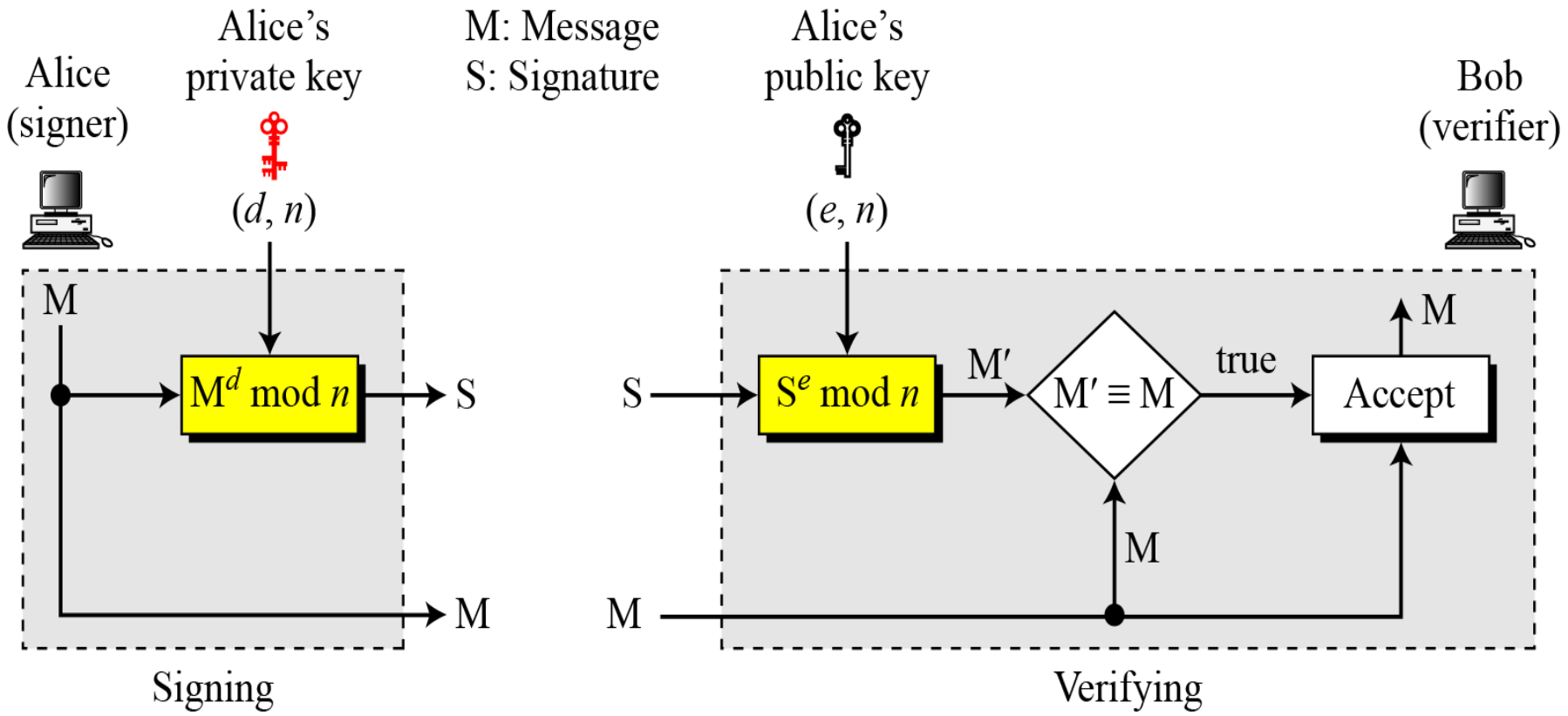
Key generation in the RSA digital signature scheme is exactly the same as key generation in the RSA

Note

In the RSA digital signature scheme, *d* is private; *e* and *n* are public.

Signing and Verifying

RSA digital signature scheme



1. Continued

Example .1

As a trivial example, suppose that Alice chooses p = 823 and q = 953, and calculates n = 784319. The value of $\phi(n)$ is 782544. Now she chooses e = 313 and calculates d = 160009. At this point key generation is complete. Now imagine that Alice wants to send a message with the value of M = 19070 to Bob. She uses her private exponent, 160009, to sign the message:

$$\text{M: } 19070 \quad \rightarrow \quad \text{S} = (19070^{160009}) \bmod 784319 = 210625 \bmod 784319$$

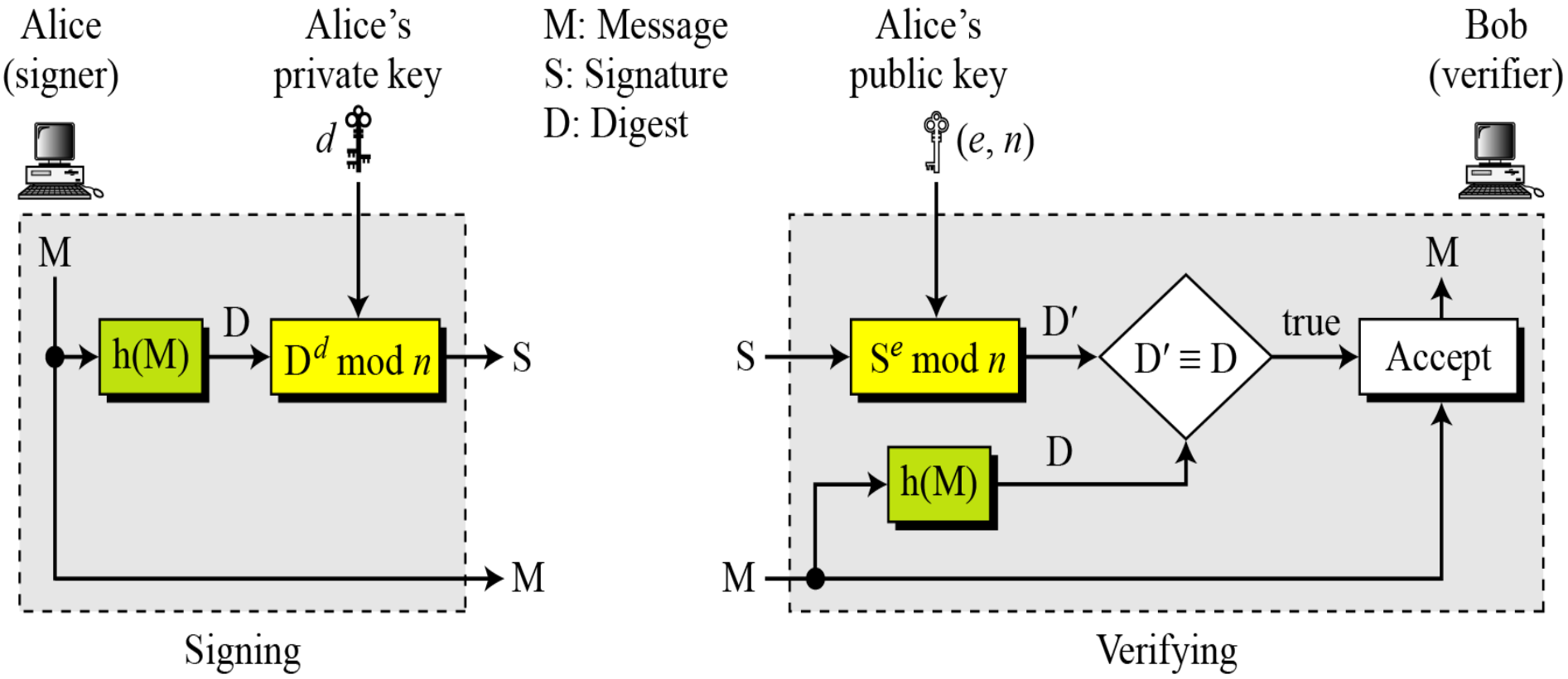
Alice sends the message and the signature to Bob. Bob receives the message and the signature. He calculates

$$\text{M}' = 210625^{313} \bmod 784319 = 19070 \bmod 784319 \quad \rightarrow \quad \text{M} \equiv \text{M}' \bmod n$$

Bob accepts the message because he has verified Alice's signature.

RSA Signature on the Message Digest

The RSA signature on the message digest



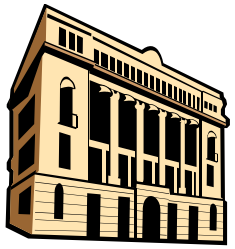
The big problem with the public key encryption and digital signature:

Is that the public key of each user has to be authenticated. (Eve should not be able to advertise her public key to the community pretending that it is Bob's public key)

This problem is solved by using digital certificate

What are Digital Certificates?

A digital certificate (DC) is a digital file that certifies the identity of an individual or institution, or even a router seeking access to computer- based information. It is issued by a Certification Authority (CA), and serves the same purpose as a driver's license or a passport.



What are Certification Authorities?

Certification Authorities are the digital world's equivalent to passport offices. They issue digital certificates and validate holders' identity and authority.

They embed an individual or institution's public key along with other identifying information into each digital certificate and then cryptographically sign with the CA's private key it as a proof seal verifying the integrity of the data within it, and validating its use.

Public-Key Certification